ЛЕКЦИЯ 5

ШИФРОВАНИЕ И ИБ

ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ) — ЭТО ОБЛАСТЬ ЗНАНИЙ И ПРАКТИЧЕСКИХ МЕТОДОВ, НАПРАВЛЕННЫХ НА **ЗАЩИТУ ИНФОРМАЦИИ** ОТ:

- КРАЖИ
- ИЗМЕНЕНИЯ
- УНИЧТОЖЕНИЯ
- НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ПРОЩЕ ГОВОРЯ: **ИБ ОТВЕЧАЕТ НА ВОПРОС — КАК СОХРАНИТЬ ДАННЫЕ БЕЗОПАСНЫМИ**.

ЗАЧЕМ НУЖНА ИБ

СЕГОДНЯ ИНФОРМАЦИЯ — ЭТО ЦЕННОСТЬ:

- БАНКОВСКИЕ ДАННЫЕ
- ПАРОЛИ
- ЛИЧНЫЕ ПЕРЕПИСКИ

- КОРПОРАТИВНЫЕ СЕКРЕТЫ
- ГОСУДАРСТВЕННЫЕ СИСТЕМЫ

БЕЗ ИБ ВОЗМОЖНЫ:

- УТЕЧКИ ДАННЫХ
- ФИНАНСОВЫЕ ПОТЕРИ

- ВЗЛОМ АККАУНТОВ
- ОСТАНОВКА БИЗНЕСА
- КИБЕРШПИОНАЖ

ОСНОВНЫЕ ЦЕЛИ ИБ

КОНФИДЕНЦИАЛЬНОСТЬ (CONFIDENTIALITY)

ИНФОРМАЦИЯ ДОСТУПНА ТОЛЬКО ТЕМ, КОМУ РАЗРЕШЕНО.

ПРИМЕР: ПАРОЛЬ ЗНАЕТ ТОЛЬКО ВЛАДЕЛЕЦ.

ЦЕЛОСТНОСТЬ (INTEGRITY)

ДАННЫЕ НЕЛЬЗЯ ИЗМЕНИТЬ НЕЗАМЕТНО.

ПРИМЕР: БАНКОВСКИЙ ПЕРЕВОД НЕ ДОЛЖЕН ИЗМЕНИТЬСЯ ПО ПУТИ.

ДОСТУПНОСТЬ (AVAILABILITY)

ИНФОРМАЦИЯ ДОСТУПНА ТОГДА, КОГДА НУЖНА.

ПРИМЕР: САЙТ БАНКА РАБОТАЕТ 24/7.

ЧТО ТАКОЕ ШИФРОВАНИЕ

ОСНОВНЫЕ ПОНЯТИЯ:

- **ОТКРЫТЫЙ ТЕКСТ** — ИСХОДНОЕ СООБЩЕНИЕ
- **ШИФРТЕКСТ** — ЗАШИФРОВАННЫЕ ДАННЫЕ
- **КЛЮЧ** — СЕКРЕТНЫЙ ПАРАМЕТР ДЛЯ ШИФРОВАНИЯ
- **АЛГОРИТМ** — МАТЕМАТИЧЕСКИЙ МЕТОД ПРЕОБРАЗОВАНИЯ

ЧТО ТАКОЕ ШИФРОВАНИЕ

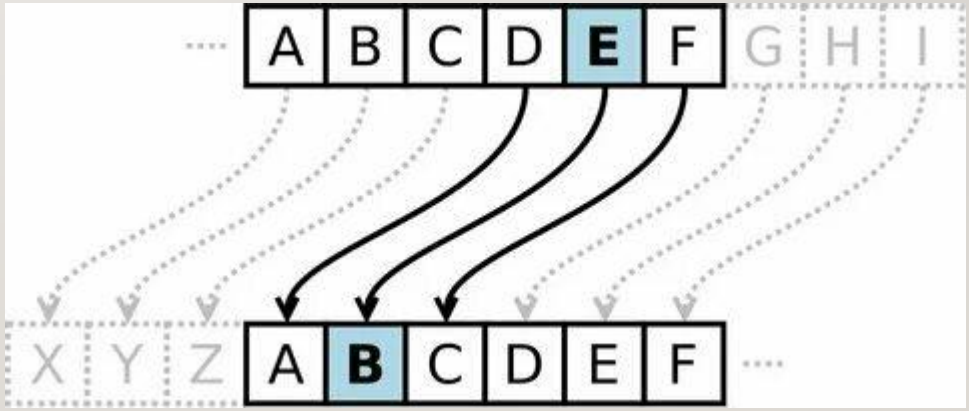
ШИФРОВАНИЕ — ЭТО ПРОЦЕСС ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ В ВИД, КОТОРЫЙ НЕВОЗМОЖНО ПРОЧИТАТЬ БЕЗ СПЕЦИАЛЬНОГО КЛЮЧА.

ИСХОДНЫЕ ДАННЫЕ → **ШИФРОВАНИЕ** → ШИФРТЕКСТ
ШИФРТЕКСТ → **РАСШИФРОВКА** → ИСХОДНЫЕ ДАННЫЕ

ПРОСТЫЕ МЕТОДЫ ШИФРОВАНИЯ

3.1 ШИФР ЦЕЗАРЯ

СУТЬ: КАЖДАЯ БУКВА СДВИГАЕТСЯ НА ФИКСИРОВАННОЕ ЧИСЛО ПОЗИЦИЙ.



ПРОСТЫЕ МЕТОДЫ ШИФРОВАНИЯ

3.2 ШИФР ПОДСТАНОВКИ

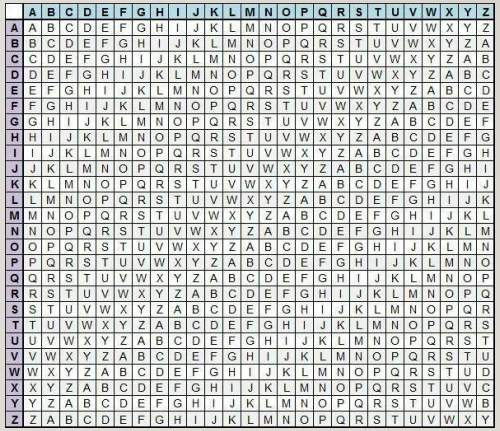
КАЖДОЙ БУКВЕ СООТВЕТСТВУЕТ ДРУГАЯ БУКВА.

ПРОСТЫЕ МЕТОДЫ ШИФРОВАНИЯ

3.3 ШИФР ВИЖЕНЕРА

ИСПОЛЬЗУЕТСЯ **КЛЮЧЕВОЕ СЛОВО**.

КАЖДАЯ БУКВА ШИФРУЕТСЯ РАЗНЫМ СДВИГОМ.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y